

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Samsung Galaxy S10, Model SM-6975,
IMEI 351751103119676

Case No.

3:19 mj 496

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-1

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

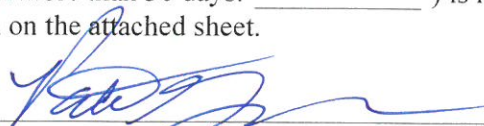
Code Section
18 U.S.C. § 922(g)(3)
18 U.S.C. § 922(a)(6)
18 U.S.C. § 924(a)(1)(A)
18 U.S.C. § 1001
21 U.S.C. § 844

Offense Description
Possession of a firearm by an unlawful user of a controlled substance or by a person addicted to a controlled substance
false statement regarding firearms
false statement regarding firearms
false statement
unlawful possession of a controlled substance

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

P. Andrew Gragan, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 08/09/2019


Judge's signature

Hon. Michael J. Newman, U.S. Magistrate Judge
Printed name and title

City and state: Dayton, Ohio

ATTACHMENT A-1

The property to be searched is a Samsung Galaxy S10, Model SM-6975, IMEI 351751103119676 cellphone, hereinafter the “Device 1,” depicted in the photographs below. Device 1 is currently located at the FBI – Dayton Resident Agency, located at 7747 Clyo Road, Centerville, Ohio.

This warrant authorizes the forensic examination of Device 1 for the purpose of identifying the electronically stored information described in Attachment B.



ATTACHMENT B

1. All records on the Devices described in Attachment A-1 and A-2 that relate to violations of:

- 18 U.S.C. § 922(g)(3)
- 18 U.S.C. § 922(a)(6)
- 18 U.S.C. § 924(a)(1)(A)
- 18 U.S.C. § 1001
- 21 U.S.C. § 844

and involve **Ethan KOLLIE (KOLLIE)** since **2013**, including:

- a. any information related to the purchase, use, or possession of firearms;
- b. any information related to the purchase, use, or sale of controlled substances;
- c. any information related to the types, amounts, and prices of controlled substances or firearms purchased, used, or trafficked as well as dates, places, and amounts of specific transactions;
- d. any information related to sources of controlled substances or firearms (including names, addresses, phone numbers, or any other identifying information);
- e. any information recording **BETTS'** schedule or travel from 2013 to the present;
- f. all bank records, checks, credit card bills, account information, and other financial records.
- g. records of Internet Protocol addresses used;

h. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
SAMSUNG GALAXY S10 MODEL SM-
6975 IMEIE 351751103119676 AND HP
LAPTOP S/N CND7110Y3L THAT ARE
STORED AT PREMISES CONTROLLED
BY THE FEDERAL BUREAU OF
INVESTIGATION

Case No. _____

3:19mj496

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, P. Andrew Gragan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), Cincinnati Division. I have been employed as a Special Agent with the FBI since May 2016. I have received training in national-security investigations and criminal investigations, and I have conducted investigations related to international terrorism, white-collar crimes, drug trafficking, public corruption, and violent crimes. As part of these investigations, I have participated in physical surveillance and records analysis, worked with informants, conducted interviews, served court orders and subpoenas, and executed search warrants.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, officers, and witnesses. This affidavit is

intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is:

- a Samsung Galaxy S10, Model SM-6975, IMEI 351751103119676, hereinafter “Device 1” (also described in Attachment A-1);
- an HP Laptop, S/N CND711OY3L, hereinafter “Device 2” (also described in Attachment A-2).

Device 1 and Device 2 (collectively referred to as the “Devices”) are currently located at the FBI – Dayton Resident Agency, located at 7747 Clio Road, Centerville, Ohio.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On or about August 4, 2019, agents with the FBI and ATF (Bureau of Alcohol, Tobacco, Firearms and Explosives) interviewed **Ethan KOLLIE (KOLLIE)**, at his residence of 1216 Cloverfield Avenue Apartment D, Kettering, Ohio, in connection with the mass shooting earlier that day in Dayton, Ohio, committed by **Conner Stephen BETTS (BETTS)**. **KOLLIE** indicated that he liked guns and currently owns a handgun and a micro Draco pistol. He also indicated that he purchased body armor and a firearm accessory for **BETTS** earlier this year. **KOLLIE** consented to a search of his residence. While inside, the agents smelled marijuana and observed, in plain sight, paraphernalia consistent with smoking marijuana including what

appeared to be a “bong,” a drug delivery device commonly used to smoke marijuana. Agents also observed in plain sight, on the counter, what they believed to be the Draco pistol. **KOLLIE** indicated that his handgun was in his bedroom.

7. On or about August 8, 2019, agents with the FBI again interviewed **KOLLIE**, this time at his place of work. **KOLLIE** advised the FBI that he was concealed carry, which based upon my training and experience is an indication that he was carrying a firearm, and that he was claiming to have a permit to do so. The FBI observed a belt clip of what appeared to be an inside-the-waistband holster. **KOLLIE** informed the FBI that he and **BETTS** had done “hard drugs,” marijuana, and acid together four to five times a week during 2014 to 2015. When asked how often he used drugs in the past year and a half, **KOLLIE** indicated that he smoked marijuana every day and had done so since he was fourteen. Agents asked **KOLLIE**: “So you never stopped,” or words to that effect. **KOLLIE** responded “that’s right,” or words to that effect. Based on my training and experience, and information from other law enforcement agents and officers, I am aware that marijuana is a controlled substance. The interviewing agents asked **KOLLIE** for consent to search his cellphone, but **KOLLIE** refused to give consent. Based on my training and experience, I know that individuals who use controlled substances, such as marijuana, use cellphones for purposes of buying controlled substances, communicating with their supplier, and storing contact information pertaining to their supplier, among other data items related to controlled substances.

8. Records obtained from a Dayton area Federal Firearm Licensed dealer included an ATF Form 4473, which based on my training and experience I know is required in order to complete the transaction of purchasing a firearm from a licensed dealer. The form pertained to the purchase by **KOLLIE** of a Century Arms Draco 7.62x39mm pistol with serial number PMD-

11797-19. The form transferee/buyer was listed as **Ethan William KOLLIE** with the address of 1216 Cloverfield Avenue, Apartment D, Kettering, Ohio, and a date of birth and social security number that is consistent with Ohio Bureau of Motor Vehicle records for **KOLLIE**. The transfer of the firearm from the dealer to **KOLLIE** was completed on May 9, 2019.

9. Box 11e of the ATF Form 4473 states, “Are you an unlawful user of, or addicted to, marijuana or any depressant, stimulant, narcotic drug, or any other controlled substance? Warning: The use or possession of marijuana remains unlawful under Federal law regardless of whether it has been legalized or decriminalized for medicinal or recreational purposes in the state where you reside.” **KOLLIE**’s Form 4473 was checked “No” in response to the question in box 11e.

10. On or about August 8, 2019, the FBI executed a federal search warrant, issued on or about August 8, 2019 by the United States District Court of the Southern District of Ohio, on the person of **KOLLIE**. When encountered by the FBI, **KOLLIE** was advised of the federal search warrant and that he was not under arrest. When asked if he had anything on his person, **KOLLIE** indicated that he had a bag of weed and a firearm. Agents pulled a small plastic bag from **KOLLIE**’s pocket, which **KOLLIE** advised was marijuana. A revolver, later identified to be a Taurus .38SPC +P with serial number GZ80488, was also removed from his person. A Samsung Galaxy S10 (Device 1) was also removed from his pocket.

11. During the execution of the warrant, the FBI asked **KOLLIE** to speak with them, and he agreed to do so. During the interview, **KOLLIE** admitted to being a regular user of illegal drugs, including marijuana and psychedelic mushrooms, which he grew in his residence. **KOLLIE** stated that he micro-doses the mushrooms on a constant basis, saying it provides him with energy and is “fun.” **KOLLIE** described the process of how he grew mushrooms in plastic

bins in his room, including the mushroom starter mycelium, the grow process, time to harvest, and the yield he obtained every two to three months. **KOLLIE** stated he had recently harvested and processed his mushrooms.

12. The FBI asked **KOLLIE** if he was asked about his drug use on the ATF form when he purchased his firearms. **KOLLIE** responded that he did remember answering that question on the ATF form when he bought his firearms. **KOLLIE** stated that he answered “no” to the questions regarding drug use. When asked why he lied on the forms, **KOLLIE** stated he knew that if he told the truth about his drug use, he would not be allowed to purchase a firearm, so he lied and answered “no.”

13. On or about August 8, 2019, the FBI executed a federal search warrant, issued on or about August 8, 2019 by the United States District Court of the Southern District of Ohio, on the premises of 1216 Cloverfield Avenue Apartment D, Kettering, Ohio. During the search of the premises, agents located the aforementioned Draco pistol, a Taurus Model PT111 G2A semi-automatic pistol with serial number TLR08219, ammunition, drug paraphernalia including a clear glass pipe and what is commonly referred to as a “bong,” and what appeared to be controlled substances, including what appeared to be mushrooms, which based on my training and experience are cultivated and consumed because they often contain psilocyn and psilocybin, Schedule I controlled substances. Agents also located an HP laptop (Device 2) from within the apartment.

14. The Devices are currently in the lawful possession of the FBI. It came into the FBI’s possession in the following way: the Devices were seized pursuant to federal search warrants, issued by the United States District Court of the Southern District of Ohio, for the person of **KOLLIE** and his residence. Therefore, while the FBI might already have all necessary

authority to search and examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

15. The Devices is currently in storage at FBI – Dayton Resident Agency located at 7747 Clyo Road, Centerville, Ohio. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing

dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- c. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media

include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

d. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I know that the Devices have capabilities that allow it to serve as a wireless telephone (Device 1), computer (both Devices),

and PDA (Device 1) that can access the internet and store internet history, IP Addresses, GPS data, communications, photos, documents, and other data. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage

medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

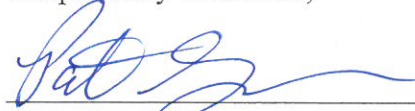
CONCLUSION

23. Based on the foregoing, I believe there is probable cause to believe that crimes have been committed, namely, violations of 18 U.S.C. § 922(g)(3) (Possession of a firearm by an unlawful user of a controlled substance or by a person addicted to a controlled substance), 18 U.S.C. § 922(a)(6) (false statement regarding firearms), 18 U.S.C. § 924(a)(1)(A) (false statement regarding firearms); 18 U.S.C. § 1001 (false statement), and 21 U.S.C. § 844

(unlawful possession of a controlled substance), and that evidence, contraband, fruits of crime, and instrumentalities of crime will be found in the Devices.

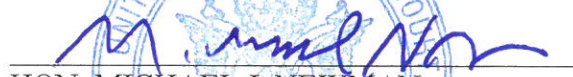
24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A-1 and A-2 to seek the items described in Attachment B.

Respectfully submitted,



P. Andrew Gragan
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on August 9, 2019, in Dayton, Ohio.


HON. MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

The property to be searched is a Samsung Galaxy S10, Model SM-6975, IMEI 351751103119676 cellphone, hereinafter the “Device 1,” depicted in the photographs below. Device 1 is currently located at the FBI – Dayton Resident Agency, located at 7747 Clio Road, Centerville, Ohio.

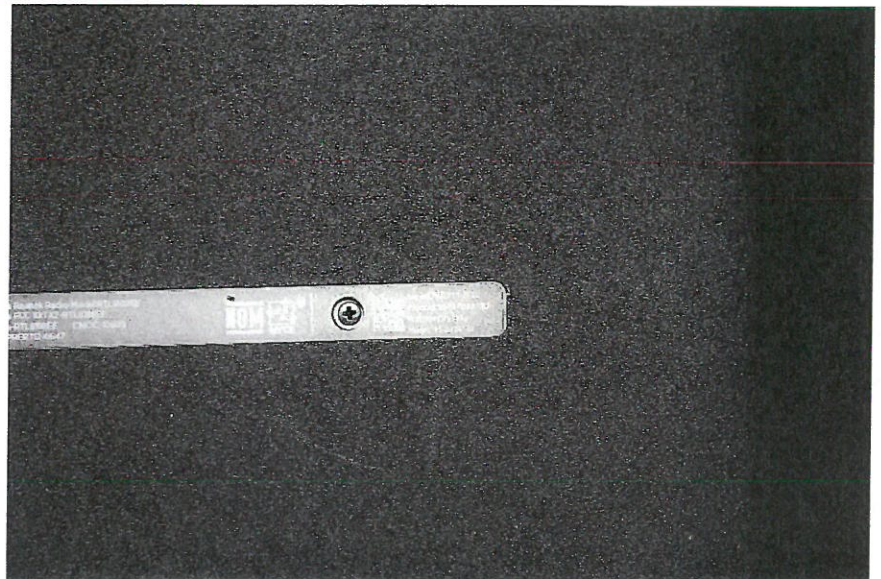
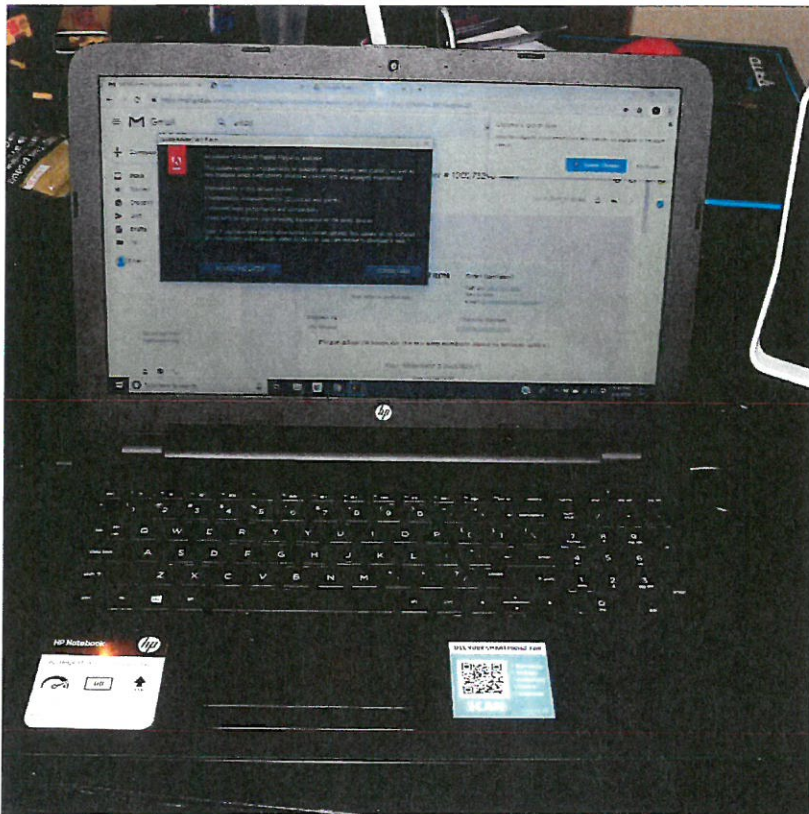
This warrant authorizes the forensic examination of Device 1 for the purpose of identifying the electronically stored information described in Attachment B.



ATTACHMENT A-2

The property to be searched is an HP Laptop, S/N CND711OY3L, hereinafter “Device 2,” depicted in the photographs below. Device 2 is currently located at the FBI – Dayton Resident Agency, located at 7747 Clys Road, Centerville, Ohio.

This warrant authorizes the forensic examination of Device 2 for the purpose of identifying the electronically stored information described in Attachment B.



ATTACHMENT B

1. All records on the Devices described in Attachment A-1 and A-2 that relate to violations of:

- 18 U.S.C. § 922(g)(3)
- 18 U.S.C. § 922(a)(6)
- 18 U.S.C. § 924(a)(1)(A)
- 18 U.S.C. § 1001
- 21 U.S.C. § 844

and involve **Ethan KOLLIE (KOLLIE)** since **2013**, including:

- a. any information related to the purchase, use, or possession of firearms;
- b. any information related to the purchase, use, or sale of controlled substances;
- c. any information related to the types, amounts, and prices of controlled substances or firearms purchased, used, or trafficked as well as dates, places, and amounts of specific transactions;
- d. any information related to sources of controlled substances or firearms (including names, addresses, phone numbers, or any other identifying information);
- e. any information recording **BETTS'** schedule or travel from 2013 to the present;
- f. all bank records, checks, credit card bills, account information, and other financial records.
- g. records of Internet Protocol addresses used;

h. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.